RECEIVED
CENTRAL FAX CENTER

FEB 20 2007

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Claims 1-17 (Cancelled).

Claim 18 (Currently Amended): A method of preventing access to code within an operational system comprising the following steps: determining at least one decryption key in a first device in response to at least one seed contained within a second device; determining ~~at least one~~ operational code for execution by [[in]] said second device in response to said at least one decryption key; and enabling the second device ~~operational system~~ to perform at least one task in response to said operational ~~at least one~~ code.

Claim 19 (Currently Amended): A method as in claim 18 wherein the step of determining at least one decryption key comprises executing an algorithm to calculate said at least one key in response to said at least one seed.

Claim 20 (Currently Amended): A method as in claim 18 wherein the step of determining ~~at least one~~ operational code comprises decrypting an encrypted operational code.

Claim 21 (Currently Amended): A method as in claim 18 further comprising the step of verifying said ~~at least one~~ operational code.

Claim 22 (Currently Amended): An operational system comprising: at least one smart device having at least one seed and encrypted code; supporting equipment determining at least one decryption key in response to said at least one seed; said at least one smart device decrypting said encrypted code in response to said at least one decryption key to generate a decrypted code; and a controller performing at least one task in response to said decrypted code.

Claim 23 (New): An operational system comprising:

a smart device comprising a first memory storing a first seed and first encrypted operational code, and a controller for causing said smart device to perform a task in accordance with the operational code only if the operational code has been decrypted;

a first key-determinative device that determines a first decryption key in response to receipt of the first seed from the smart device and as a function of the first seed; and

a first code-determinative device that decrypts the encrypted operational code in response to receipt of the first decryption key.

Claim 24 (New): The system as in claim 23, wherein the first code-determinative device is incorporated in the smart device.

Claim 25 (New): The system as in claim 23, wherein the first code-determinative device is incorporated in the first key-determinative device.

Claim 26 (New): The system as in claim 23, wherein the smart device is a deployable device and the first key-determinative device is a launcher designed to launch the deployable device.

Claim 27 (New): The system as in claim 26, wherein the operational code is used to deploy the deployable device.

Claim 28 (New): The system as in claim 23, wherein the smart device is a computer system.

Claim 29 (New): The system as in claim 23, wherein the first key-determinative device comprises a key algorithm for determining the first decryption key.

Claim 30 (New): The system in claim 23 wherein the first key-determinative device verifies the operational code.

Claim 31 (New): The system in claim 23 wherein the first key-determinative device comprises a second memory storing a key algorithm, a second controller and a key calculator that calculates the first decryption key as a function of the first seed.

Claim 32 (New): The system as in claim 23 wherein the first seed is stored in a predetermined address in the first memory and the first key-determinative device stores an identification of the predetermined address.

Claim 33 (New): The system as in claim 23, wherein the first seed is stored in a predetermined address in the first memory and the controller does not store an identification of the predetermined address.

Claim 34 (New): The system as in claim 23, wherein the controller verifies the operational code.

Claim 35 (New): The system as in claim 23, wherein the smart device is unable to determine the first decryption key.

Claim 36 (New): The system as in claim 23, wherein the first seed is inaccessible to the controller of the smart device.

Claim 37 (New): The system as in claim 23, further comprising:

a second memory storing a second seed, the second memory being incorporated in the first key-determinative device;

a second key-determinative device that determines a second decryption key in response to receipt of the second seed and as a function of the second seed; and

a second code-determinative device that determines an identification of the address in the first memory where the first seed is stored in response to receipt of the second decryption key from the second key-determinative device.

Claim 38 (New): The system as in claim 37, wherein the second code-determinative device is incorporated in the first key-determinative device.

Claim 39 (New): The system as in claim 37, wherein the smart device is a deployable device and the operational code is used to deploy the deployable device, the second memory and the first key-determinative device are components of a launcher for the deployable device, and the second key-determinative device is part of a ground-based station.